

## ATTACHMENT A

Graphic 1:

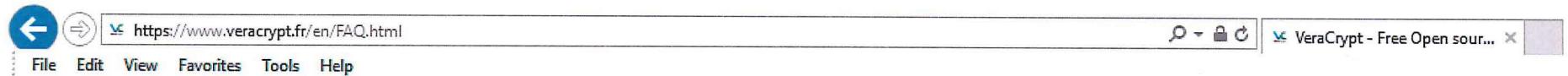
The screenshot shows a web browser window for the VeraCrypt website at <https://www.veracrypt.fr/en/Home.html>. The page features the VeraCrypt logo (a stylized 'VC' in blue and green) and the word 'VeraCrypt'. Below the logo is a navigation bar with links: Home, Source Code, Downloads, Documentation, Donate, and Forums. The 'Home' link is highlighted with a green background. The main content area contains a brief introduction: 'VeraCrypt is a free open source disk encryption software for Windows, Mac OSX and Linux. Brought to you by IDRIX (<https://www.idrix.fr>) and based on TrueCrypt 7.1a.'

Graphic 2:

The screenshot shows a web browser window for the VeraCrypt website's FAQ page at <https://www.veracrypt.fr/en/FAQ.html>. The page title is 'What's the difference between TrueCrypt and VeraCrypt?'. The text explains that VeraCrypt adds enhanced security to the algorithms used for system and partitions encryption, making it immune to new developments in brute-force attacks. It also solves many vulnerabilities and security issues found in TrueCrypt. An example is given: when the system partition is encrypted, TrueCrypt uses PBKDF2-RIPMD160 with 1000 iterations whereas in VeraCrypt we use 327661. And for standard containers and other partitions, TrueCrypt uses at most 2000 iterations but VeraCrypt uses 655331 for RIPEMD160 and 500000 iterations for SHA-2 and Whirlpool.

This enhanced security adds some delay only to the opening of encrypted partitions without any performance impact to the application use phase. This is acceptable to the legitimate owner but it makes it much harder for an attacker to gain access to the encrypted data.

### Graphic 3:



I forgot my password – is there any way ('backdoor') to recover the files from my VeraCrypt volume?

We have not implemented any 'backdoor' in VeraCrypt (and will never implement any even if asked to do so by a government agency), because it would defeat the purpose of the software. VeraCrypt does not allow decryption of data without knowing the correct password or key. We cannot recover your data because we do not know and cannot determine the password you chose or the key you generated using VeraCrypt. The only way to recover your files is to try to "crack" the password or the key, but it could take thousands or millions of years (depending on the length and quality of the password or keyfiles, on the software/hardware performance, algorithms, and other factors). Back in 2010, there was news about the [FBI failing to decrypt a TrueCrypt volume after a year of trying](#). While we can't verify if this is true or just a "psy-op" stunt, in VeraCrypt we have increased the security of the key derivation to a level where any brute-force of the password is virtually impossible, provided that all security requirements are respected.

Graphic 4:

The screenshot shows a web browser window with the URL [https://www.idrix.fr/Root/mos/Contact\\_Us/task;view/contact\\_id,1/Itemid,30/](https://www.idrix.fr/Root/mos/Contact_Us/task;view/contact_id,1/Itemid,30/). The page title is "Contact Us - IDRIX: Cryptog...". The browser's address bar also displays the URL. The page header features the IDRIX logo and the tagline "Cryptography And IT Security Experts™". The navigation menu includes links for Contact Us, Customers, Blog, and Home. A sidebar on the left contains links for Home, Products, Free Utilities, Blog, Customers, and Contact Us. The main content area shows the "Contact Us" section for Mounir IDRASSI, with contact information including an address (9 rue du Docteur Germain Sée, 75016, Paris, France), email (contact@idrix.fr), phone numbers (+33183621570, +33179756905), and a RCS Paris registration number (RCS PARIS 490 000 619). To the right of the contact information is a small map of Paris with a yellow square marker indicating the location.